View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Xiamen University Institutional Repository

学校编码：10384　　分类号＿＿＿密级＿＿＿
学号：X2007223013　　UDC ＿＿＿

厦门大学

工 程 硕 士 学 位 论 文

基于校园网的网络流量异常分析与预测

Based on Campus Network Analysis and Forecast of network traffic anomalies

郭瑞香

指导教师姓名：吴顺祥 教授
黄　轩 高级工程师

专 业 名 称：控制工程
论文提交日期：2010 年 5 月
论文答辩日期：2010 年 6 月
学位授予日期：　　年　月

答辩委员会主席：＿＿＿＿＿

评阅人：＿＿＿＿＿

2010 年 6 月

厦门大学博硕士论文摘要库

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学博硕士论文摘要库

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

摘 要

随着校园网的快速发展，校园网网络规模不断扩大,网络结构和网络设备的的日趋复杂化，以及各种新型应用不断增加，如各种 p2p 的应用，音、视频点播服务等等。网络的复杂化，对网络维护、网络管理、网络拥塞控制、网络服务质量保证等等的要求也越来越高，而另一方面校园网中的安全威胁(如 DOS、DDOS、蠕虫、恶意代码等)却越来越多。特别是面对现在网络攻击、网络病毒的广泛泛滥，以及网络故障的时常发生，如何有效的管理和控制网络，是网络流量工程面临的重要问题。种种原因需要我们对校园网流量进行时时监控，以便随时发现流量异常，及时定位引起网络异常情况的源头，有效地控制异常流量的蔓延，及时有针对性地采取措施，以避免网络阻塞。同时合理地分配带宽，保障主要业务的正常开展。

校园网中出现的网络流量异常主要由网络攻击、网络病毒、网络突发访问、网络故障、网络新用户的加入等引起，这种异常往往给网络和计算机用户带来极大损失甚至是致命危害。为了防护校园网络和个人计算机免受损害，传统的方法是采用防火墙、病毒防御技术。流量异常检测不同于传统的检测方法，它采用主动的检测方法去发现网络漏洞、网络攻击、网络病毒和网络故障，它不仅能发现已知的病毒和攻击类型，而且也能检测未知的、新的病毒和攻击类型，它采用的是一种主动防御技术。流量异常检测基于网络流量研究的最新成果，通过建立关于网络流量异常和正常的检测模型，将网络流量分为正常流量和异常流量，正常流量是合法用户的正常访问引起的流量，而异常流量则是网络攻击、网络病毒、网络故障引起的流量，异常流量是可疑流量，是网络入侵检测系统要重点分析的对象。

本文主要研究内容:

1. 本文主要从当前校园网的发展、特点分析校园网的现状，从而提出校园网的流量有效管理的迫切性；

2.从网络异常流量种类、危害性、预警及流向进行分析，根据经验提出相应的异常流量处理方法，研究学习相应的常用入侵检测方法。

厦门大学博硕士论文摘要库

3. 基于 Netflow 对校园网异常流量的特征、流向、源目的端口进行了深入分析，进而提出如何在网络层面对校园网异常流量采取防护措施，其中重点讲述了 NetFlow 分析在校园网异常流量防护中的应用及典型案例，提出基于 Netflow 的监控管理模型。

4. 经过常用路由算法比较，基于 Netflow 检测出的异常流量监测情况，运用灰色系统理论建模理论和残差修正方法，提出一种基于流量的链路状态路由改进算法。

关键词：校园网，流量异常，Netflow, 灰色神经网络， 路由

厦门大学博硕士论文摘要库

Abstract

With the rapid development of the campus network, campus network have been expanding, the network structure and network devices become more complex, and the increasing variety of new applications, such as a variety of p2p applications, audio and video on demand services, etc., in the face This complex networks, it's network maintenance, network management, network congestion control, network quality of service to ensure higher and higher demands, etc., on the other hand the campus network to security threats (for example DDOS, Worm, malicious code) But more and more. In the face of current network attacks, network viruses spread widely, and network failures frequently occur, and how to effectively manage and control network,Network traffic is an important issue facing the project. On campus for various reasons we need to constantly monitor the network traffic in order to keep traffic anomaly was found in time positioning the source of anomalies caused by the network, effectively control the spread of abnormal flow, timely, targeted measures to avoid network congestion. Have a reasonable allocation of bandwidth, to protect their main business normally.

Abnormal network traffic is network attacks, network viruses, network burst access, network failure, the network of new users join the network traffic caused by such anomalies, such anomalies are often computer users to the network and bring great loss or even fatal damage. For protection against damage to networks and personal computers, the traditional approach is to use a firewall, virus defense technology. Traffic anomaly detection are different from traditional testing method, which uses active detection method to discover network vulnerabilities, network attacks, network viruses and network failure, it can not only find the known types of viruses and attacks,But also to detect unknown and new types of viruses and attacks, it is used in an active defense technologies. Traffic anomaly detection of network traffic based on the latest achievements, through the establishment of network traffic anomalies and normal detection model, the network traffic into normal and abnormal

厦门大学博硕士论文摘要库

traffic flow, the normal flow of legitimate users to access due to the normal flow, and abnormal traffic is is a network attack, network viruses, network failure caused by flow, abnormal flow is suspicious traffic, network intrusion detection system is to focus the analysis objects.

This paper mainly studies the content:

1. This article mainly from the current development of campus network, the characteristic analysis of the present situation, and proposed the campus

Net flow of effective management of urgency,

2 from the network traffic types, harmfulness and abnormal warning and flow analysis, according to the experience of the corresponding treatment method, abnormal flow study corresponding common intrusion detection methods.

3 Netflow based on campus network traffic flow characteristics of abnormal, source, analyses the destination portAnalysis, then puts forward how to network of campus network anomalies in the protective measures, including traffic NetFlow focused on the analysis of network flow anomalies in the application and the typical case protection, based on the NetFlow monitoring management model.

4 after routing algorithm based on comparative, used to detect abnormalities Netflow flow monitoring situation, the modeling theory of grey system theory and residual correction method, is proposed based on the flow of link-state routing algorithm.

Keywords: The campus net; traffic abnormity;NetFlow; Grey Neural Network ;Routing

厦门大学博硕士论文摘要库

目 录

摘 要 I

Abstract III

第一章 绪论 1

1.1 当前校园网的发展状况 1

1.2 校园网络的特点及安全现状分析 1

1.3 进行网络流量有效管理的迫切性 6

1.4 网络流量管理的发展趋势 8

1.5 论文的研究目的和意义 8

1.5.1 论文的研究目的 8

1.5.2 研究意义 8

第二章 网络流量异常的检测技术 11

2.1 网络流量异常的种类 11

2.1.1 异常流量的分类 11

2.1.2 异常流量的危害性 15

2.1.3 异常流量的预警 16

2.1.4 异常流量的处理及方法 17

2.2 异常流量流向分析 18

2.3 异常流量的常用入侵检测方法 19

2.4 本章小结 20

第三章 一种基于 NET FLOW 的网络异常的检测方法 21

3.1 Net Flow 的概念与原理 21

3.1.1 Net Flow 的概念 21

3.1.2 Net Flow 的基本原理 21

3.1.3 校园网中 Net Flow 的配置 24

3.2 数据流采集技术 25

3.2.1 流量采集方式的比较 25

厦门大学博硕士论文摘要库

3.2.2 利用 NetFlow 数据采集 27
3.2.3 NetFlow 数据格式 29
3.3 校园网的异常流量的 Net Flow 分析 **29**
3.3.1 异常流量流向分析 30
3.3.2 利用 Net Flow 分析出异常流量 31
3.3.3 异常流量的源、目的地址 31
3.3.4 异常流量的源、目的端口分析 32
3.4 基于 NetFlow 的监控管理模型 **32**
3.5 常见蠕虫病毒的 NetFlow 分析案例 **34**
3.6 NetFlow 的校园网应用 **35**
3.7 本章小结 **37**
第四章 基于灰色神经网络流量预测的路由算法 **39**
4.1 灰色系统理论的基本原理和方法 **39**
4.2 路由概述 **40**
4.3 常用路由算法的比较 **40**
4.3.1 洪泛法（Flooding） 40
4.3.2 随机走动法（Random Walk） 40
4.3.3 链路状态路由算法 41
4.4 基于流量的路由选择 **43**
4.5 基于流量的链路状态路由算法 **44**
4.5.1 网络节点流量预测算法 44
4.5.2 最佳路由选择新算法描述 44
4.6 本章小结 **45**
第五章 总结与展望 **46**
5.1 论文研究总结 **43**
5.2 论文研究展望 **44**
参考文献 **48**
致谢 **51**

厦门大学博硕士论文摘要库

Contents

Abstract ……..I

Abstract

……II

I

Chapter 1 Introduction.....1

1.1 The development situation of campus network.....1

1.2 Campus network and the characteristics of the current safety analysis.....1

1.3 Network flow of effective management of urgency.....6

1.4 The development trend of the management of network traffic.....8

1.5 The paper studies purpose and meaning.....8

1.5.1 The research papers.....8

1.5.2 Research significance.....8

Chapter 2 Network flow anomalies detection technology.....**11**

2.1 Network flow types of abnormal.....11

2.1.1 The classification of abnormal flow.....11

2.1.2 The harmfulness of flow anomalies.....15

2.1.3 Warning of The abnormal flow.....16

2.1.4 Abnormal flow processing and methods.....17

2.2 Abnormal discharge flow analysis.....18

2.3 Abnormal flow of common intrusion detection methods.....19

2.4 Summary.....20

Chapter 3 A method based on the Net Flow network anomaly detectionmethods ……21

3.1 The concept and principle NetFlow.....21

3.1.1 NetFlow concept.....21

3.1.2 The basic principle of net Flow.....21

3.1.3 Network Flow in the.net configuration.....24

3.2 Data collection technology.....25

3.2.1 Traffic acquisition method.....25

3.2.2 Use NetFlow data acquisition.....27

厦门大学博硕士论文摘要库

3.2.3 NetFlow data formats.....29
3.3 Campus network Flow analysis of asp.net abnormal Flow.....29
3.3.1 Abnormal discharge flow analysis.....30
3.3.2 Using asp.net Flow analysis the abnormal Flow.....31
3.3.3 The source, abnormal flow.....31
3.3.4 Abnormal flow sources, the destination port.....32
3.4 Based on the NetFlow monitoring management model.....32
3.5 Common NetFlow of worm virus case analysis.....34
3.6 NetFlow network applications.....35
3.7 Summary.....37
Chapter 4 Based on neural network traffic prediction of grey routing algorithm 39
4.1 The gray system theory, the basic principle and method.....39
4.2 Summary routing.....40
4.3 The routing algorithm used.....40
4.3.1 Flooding.....40
4.3.2 Random Walk.....40
4.3.3 Link-state routing algorithms.....41
4.4 Based on the flow routing.....43
4.5 Based on the flow of link-state routing algorithms.....44
4.5.1 Network node flow prediction algorithm.....44
4.5.2 The best routing algorithm.....44
4.6 Summary.....45
Chapter 5 Conclusions and Expectation.....46
5.1 Conclusions.....43
5.2 Research prospect.....44
References.....48
Acknowledgments..... 51

厦门大学博硕士论文摘要库

第一章 绪论

1.1 当前校园网的发展状况

校园网建设于1993年，分布的PC之间采用10/100M以太网技术作为联接通道， 2000年后，校园网进入了第二个发展阶段，千兆以太网的接入带动了校园网的应用发展，多媒体教学、办公自动化、网络图书馆、校园一卡通、远程教育系统、流媒体下载等应用出现，网络已经成为高校教育的一个不可或缺的平台。校园网不再仅仅是将学校“接入”网络，而是尽可能地将学校的运作“搬”到网上来，实现校园教学、科研、后勤等各个领域的“数字化”。把校园“搬”上网络，让数字“走”进生活，已成为我国越来越多高校和中小学校的选择。目前，在计算机网络建设大潮中，走在前列的是高校的计算机网络。高校校园网的建设是随着中国教育和科研计算机网(CERNET)的发展而建设起来的，中国教育和科研计算机网的建设是1993年启动的，在很短的时间内发展成为我国四大骨干网中真正由各个园区网(校园网)组成的节点数众多的计算机网络，校园网是中国教育和科研计算机网(CERNET)的重要组成部分。随着教育部“211”工程的推进，加快了教育科研网的建设步伐，在1995年底，就有108所院校接入了中国教育和科研计算机网，并初步建设了自己的校园网，在以后的几年中，中国教育和科研计算机网的发展十分迅速。这些院校大多数都建立了比较完善的计算机网络，那些建设网络较早的院校，在这几年中也经过了多次改造，现在都已经具有了较好的网络基础设施。高校是人员密集型地区，少则近万人，多则几万人，而且学生和教师都使用网络频繁的人群，因而校园网内的联网主机发展的极为迅速，使得校园网内的节点数变得十分庞大。截止目前，覆盖全国31个省（自治区、直辖市）的200多座城市，联网单位1500多个，用户1800多万，成为国内仅次于中国电信的第二大互联网络。

1.2 校园网络的特点及安全现状分析

随着校园网规模不断扩大，网络结构越来越复杂，信息系统越来越多，数据

越来越丰富用户越来越多，面临的问题和风险也越来越多，网络服务也越来越多样化。目前的校园网有拨号认证网络、无线网络、专线网络等多种网络。采用的网络技术包括快速以太网技术、ATM 技术、WLAN 技术、VLAN 技术等。校园网络在提供传统 Internet 服务的基础上，网络应用越来越丰富多彩，不仅包括电子邮件、WWW, FTP, DNS、虚拟主机、信息搜索等传统服务，也包括 VOD 视频点播、视频会议等多媒体服务和图书馆信息服务等等,但随着其应用的深入，校园网络的安全问题也逐渐突出，令网络管理着烦恼的事也接踵而来：用户非法接入网络或者肆意修改 IP 地址，在网络论坛上留下非法言论，利用协议漏洞的 ARP 欺骗导致网络业务中断，这些种种安全方面直接影响着学校的教学、管理、科研活动。因此，在全面了解校园网的安全现状基础上，合理构建安全体系结构，改善网络应用环境的工作迫在眉睫[34].

在调查中，84.19%的学校校园网主干带宽在千兆以上，百兆带宽到桌面的占86.23%,校园网带宽需求日增,千兆带宽百兆到桌面已渐普及.在提供服务时遇到的问题方面,44.44%的学校选择了带宽瓶颈,33.76%的学校选择远程接入安全问题 26.50%选择服务器压力过大.带宽瓶颈已成为校园网提供服务的最大问题.说明了校园网用户越来越多.网络建设方面,在主要的促动因素方面,网络安全需求,信息化建设和应用需求成为重要的推动力量.调查中,141 个学校首选了网络安全需求,占 60.26%(如图 1.1)

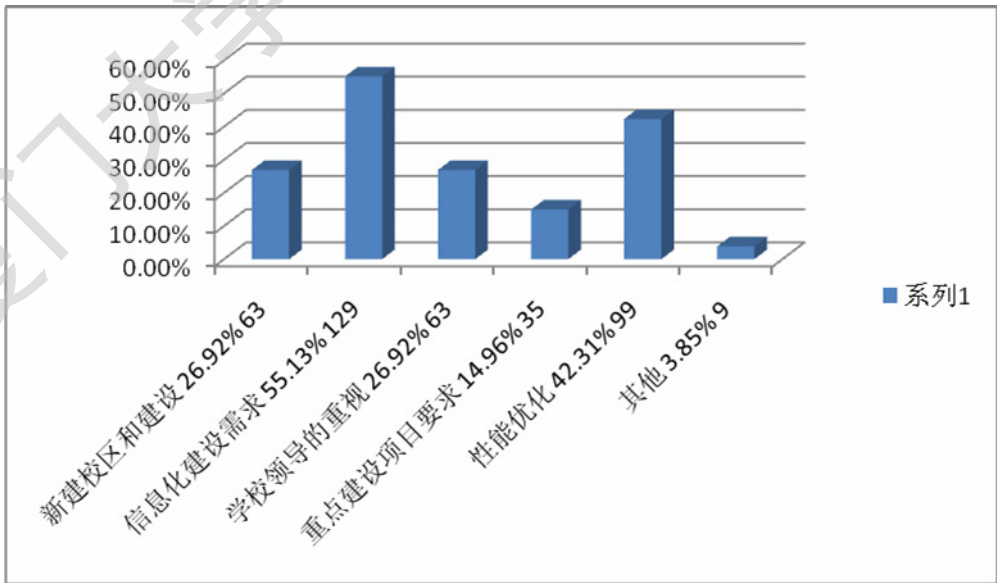

图 1.1 网络建设主要的促动因素

在校园网建设中，病毒防治、数据安全仍是高校网络建设关注的重中之重，

70.09%选择病毒防治，66.24%的学校选择数据安全，近年来，校园网安全事故频频发生，威胁到校园网数据信息安全有很大关系。如图 1.2

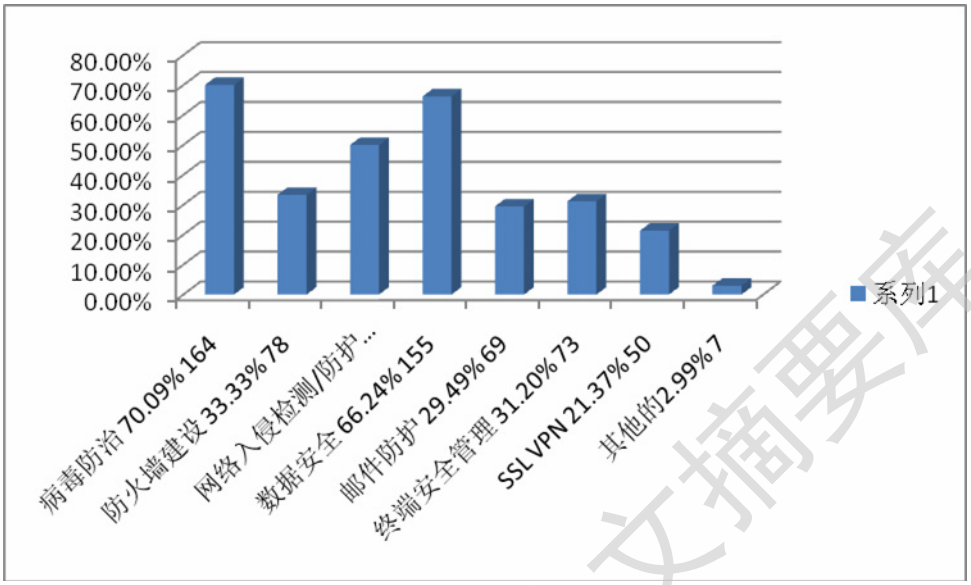

图 1.2 校园网建设中最关注的安全问题

校园网的网络安全有其独特性，近年来，各种安全事件逐渐趋利化，攻击对象也向终端转移，大大小小的安全事件不断冲击校园网。在调查中，近一年来发生过网络安全的学校占 60%以上，发生安全事件种类繁多，其中，感染病毒、蠕虫、木马程序、恶意代码等，未授权访问或拒绝服务攻击（DOS），网页被篡改等三个方面是校园网安全重点（如图 1.3）

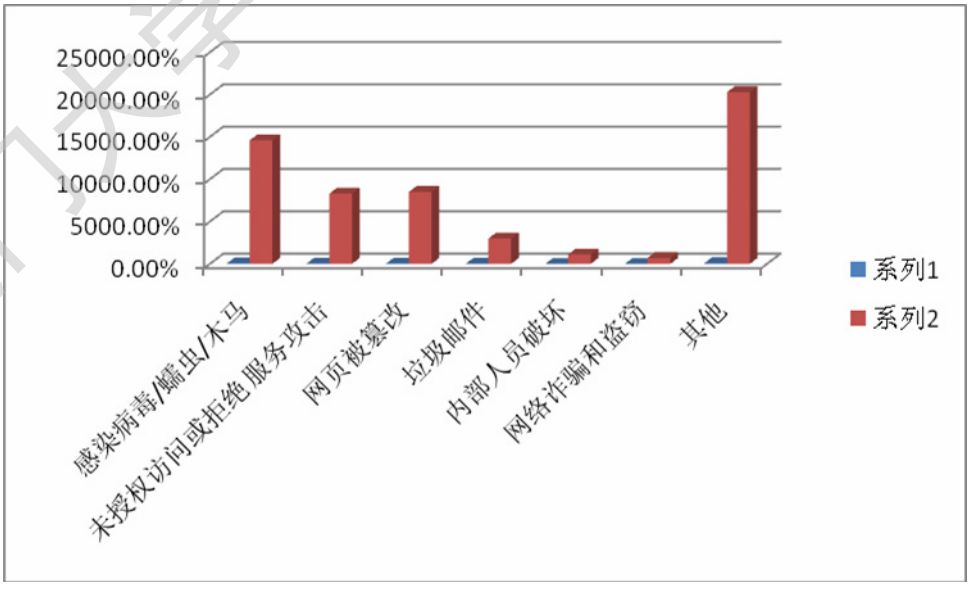

图 1.3 网络安全类型

校园网具有开放、高带宽、多主机、安全度低等特点，一般都是采用最先进

的设备和网络技术,网络应用普及,用户群密集而且活跃,容易被入侵和利用的对象，因此安全问题比较突出,安全管理更为复杂、困难，虽校园网的建设给学校的教学和管理、学生的学习等多方面带来了很大促进，但是，随着校园网上的各种数据的急剧增加,各种各样的安全问题接踵而来。目前,导致高校校园网络安全事件的原因很多，主要包括一下几个方面[34]：

(1)网络或系统的漏洞，对信息安全、系统的使用、网络的运行构成严重的威胁。

(2)网络或软件配置错误。

(3)计算机蠕虫、病毒泛滥，影响用户的使用、信息安全、网络运行。

(4)外来用户系统入侵、攻击等恶意破坏行为，部分计算机已经被攻破，用作黑客攻击的工具;拒绝服务攻击目前越来越普遍，不少开始针对高校的网站和服务器。

(5)校园网内部攻击行为,校园网内部也存在很大的安全隐患,由于内部用户对网络的结构和应用模式都比较了解,因此来自内部的安全威胁更难应付。

(6)校园网内部资源的滥用，有的校园网用户利用免费的校园网资源提供商业的或者免费的视频、软件资源下载，占用了大量的网络带宽，影响了校园网的应用。

(7)垃圾邮件、不良信息的传播，有的利用校园网内无人管理的服务器作为中转，严重影响学校的声誉。

(8) 安全管理不到位。校园网的用户群体大,少则数千人、多则数万人,数据量大、速度高。随着校园内计算机应用的大范围普及,接入校园网节点日渐增多,学生通过网络在线看电影、听音乐,很容易造成网络堵塞和病毒传播。而这些节点大部分都没有采取一定的防护措施,随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。

（9）硬件系统的安全威胁。硬件的安全问题也可以分为两种,一种是物理安全,一种是设置安全。

校园网既是许多网络攻击的发源地，也是攻击者最容易攻破的目标。“三分技术，七分管理“，这是学校网络建设和管理着常挂嘴边的一句话，目前，校园网的现状分析如下[34]：

厦门大学博硕士论文摘要库

Degree papers are in the “Xiamen University Electronic Theses and Dissertations Database”. Full texts are available in the following ways:
1. If your library is a CALIS member libraries, please log on http://etd.calis.edu.cn/ and submit requests online, or consult the interlibrary loan department in your library.
2. For users of non-CALIS member libraries, please mail to etd@xmu.edu.cn for delivery details.

厦门大学博硕士论文摘要库